

**Remarks**

In the interest of clarity the paragraph numbers and title below mirror the substantive paragraph numbers and title in the Office Action.

As an initial matter Applicant describes the present invention in basic terms which Applicant believes will help in determining the scope of the claims. To this end, it has been recognized that, often, medical facilities employ software programs from many different vendors and that those programs often use different types of patient identification numbers. For instance, a first software application program may use patient social security numbers to distinguish patients, a second program may use a simple six digit numbering system to distinguish patients (e.g., 111111; 111112; 111113, etc.), a third program may use a combination of ten numbers and letters (e.g., 1121kkl1m; 3442sdfo9d; etc.), and so on.

Where different applications use different numbers to refer to the same patient, problems can arise when a first application requires information from a second application for a specific patient. For instance, where a first application program uses ID number 111111 to refer to a first patient and a second application uses ID number 3442sdfo9d to refer to the first patient, when the first application needs information from the second application regarding the first patient, the first program may only be able to formulate a query including the ID number 111111 which cannot be understood by the second application (i.e., the second application only recognizes number 3442sdfo9d as an identifier of the first patient).

One solution to this problem would be to provide a system wherein each application program stores a database including a list of network applications and application and patient distinct patient identification numbers associated with each application. Here, when the first application program needs a record for a first patient from a second application program, the first program can formulate a request using the patient identification number associated with the first patient that is used by the second application. In the alternative, where the first application program transmits a request to the second application program using the patient identification number for the first patient

that is used by the first application program, the second application program could be programmed to use the patient identification number to identify the patient identification number used by the second application program. In either of these two cases the maintenance requirements to maintain separate instances of the application-patient identification number database at each of the applications (e.g., perhaps 100 different applications on a network) would be daunting and relatively expensive and therefore these solutions to the problem are not very good.

According to the present invention a clinical exchange server is provided that enables communication between multiple application programs, each of which uses an application distinct patient identification number for each separate patient. To this end, the clinical exchange server maintains a patient identification number reference table or the like that includes a list of applications on a network and patient identification numbers used by each of the applications wherein the patient identification numbers are application distinct numbers for the patients. Thus, the patient identification numbers are both patient and application distinct.

In the above example, the patient identification number reference table would list each of the first and second applications (along with any other network applications) and would also list the application distinct patient identification numbers for each patient including the first patient. Consistent with the above, the listed patient identification numbers for the first patient would include 111111 corresponding the first application and 3442sdfo9d corresponding to the second application (and other application distinct identification numbers for the first patient).

Continuing with the above example, when the first application needs to obtain information about the first patient from the second application, the first application generates a query using the first patient ID number 111111 and sends that query to the clinical exchange server. Upon receiving the query, the server recognizes that the query is to be directed to the second application, uses number 111111 to identify identification number 3442sdfo9d corresponding to the second application and generates a query to the second application using number 3442sdfo9d which, when the query is received by the second application, is recognized by the second application as

referencing the first patient.

Consistent with the above, claim 1 requires, among other things, a clinical exchange server programmed (i) to maintain a patient identification cross reference table, the reference table including a list of applications on the network and patient identification numbers used by each application wherein the patient identification numbers used by the applications are application distinct numbers for the patient, (ii) to maintain a list of events reported to it by other applications on the network and (iii) to respond to inquiries from a first application about an event recorded by a second application by transmitting a query to the second application based on the information in the reference table and the list of reported events.

1. The Office Action rejected each of claims 1-8 as indefinite because claims 1 and 5 each include the language “wherein at least a subset”. Applicant has amended each of claims 1 and 5 to eliminate the language that was rejected.

2. The Office Action rejected each of claims 1-8 as obvious over Morange in view of Felsher. Applicant strongly traverses this rejection. Claim 1 requires, among other things, a clinical exchange server programmed (i) to maintain a patient identification cross reference table, the reference table including a list of applications on the network and patient identification numbers used by each application wherein the patient identification numbers used by the applications are application distinct numbers for the patient and to respond to inquiries from a first application about an event recorded by a second application by transmitting a query to the second application based at least in part on the information in the reference table. Neither Morange nor Felsher teach or suggest an exchange server that maintains a reference table that includes patient and application distinct patient identification numbers.

As an initial matter a summary of how Felsher teaches records are requested by a system user (i.e., a record recipient) and how the system encrypts, transmits and decrypts the records is instructive. In this regard Felsher teaches that a user (i.e., a recipient or medical professional) can use a workstation 12 (see Fig. 1) to request a

record associated with a specific patient from a server 3/5 that is associated with a medical information database 6. To identify a specific patient in a request, the request includes a system wide patient identification number such as a social security number or the like (see paragraph 266).

When a request is received, assuming that the requesting user has the right to access the requested record, the server 3 obtains the record and then uses a public key associated with the requesting user (i.e., associated with a medical professional) to encrypt the record prior to transfer (see paragraphs 220, 228, 238, 242 and 252). Because the system wide patient ID number is part of the record, the patient ID number is encrypted. The public key is recipient (i.e., medical professional) distinct (see paragraphs 220 and 269). The encrypted record is transmitted to the recipient (i.e., the medical professional) along with an applet which is a program that is usable by the recipient's workstation to decrypt the encrypted record (see paragraph 252).

In addition to requiring the applet to decrypt the encrypted record, the recipient's workstation also requires a recipient specific or distinct private key which, as the label implies, is private or known only to the recipient's (i.e., the medical professional's) workstation (see paragraph 269). The applet is not recipient distinct – i.e., the same applet is transmitted with each encrypted record irrespective of which recipient the record is transmitted to and irrespective of which application was used to access the record. Here, the private key is associated with the medical professional recipient's computer account so that the private key “follows” the user around and is available irrespective of which workstation or other device the recipient employs to access the system.

Once the recipient's workstation receives the encrypted record and the applet, the workstation decrypts the record using the private key and the applet and uses the information in the decrypted record accordingly. Here, after decryption, the patient ID is identical to the patient ID in the original record at the server.

Thus, Felsher's private keys are only associated with system users (e.g., medical professionals) and are not stored in a central exchange server and the applets are not application distinct (i.e., the same applet is transmitted with each transmitted record

irrespective of which application is used to access the record). Because the applets are not application distinct and the private keys are not stored in an exchange server table (i.e., the private key is private), the applet and private key cannot possibly be combined to teach or suggest application distinct patient identification numbers for each application on a network in an exchange server table as required by claim 1.

In addition, Felsher's private keys are not application specific keys. To this end, private keys are recipient (i.e., system user) distinct (see paragraph 269) which is different than application specific. For instance, where a first physician uses multiple different application programs to access a patient record in Felsher, the physician only has a single private key used to decrypt received records irrespective of which application program is used to access the record. As an example, where a first physician accesses a first patient record using a first application and then uses a second application to access the first patient record at a later time, each time, irrespective of which application is employed to access the record, the first physician's single private key is used to decrypt.

As another instance, where two different physicians use the same application program to access a first patient record, each physician has his own private key despite the fact that only a single application is employed to access. Thus, private keys are recipient specific and not application specific.

Therefore, private keys are recipient distinct, not application distinct, the applets are not application distinct and therefore the combination of a private key and an applet cannot possibly be application specific.

A more persuasive but yet still flawed application of Felsher to the claim 1 invention would rely on the public keys that are used to encrypt records (including uniform patient identification numbers (i.e., SS numbers) prior to transmission to recipients. To this end, Felsher teaches that separate/unique public keys are maintained by server 3 for each system user that is authorized to access system records (i.e., record recipients) (see paragraph 220). When a system user requests a

record, Felsher teaches that a system server accesses the user's unique public key, uses the public key to encrypt the record and transmits the encrypted record to the requesting user. Thus, the system server maintains a list of public keys for each system user that can access system records.

Despite the fact that Felsher's public keys are maintained by a central server, the public keys suffer from the same shortcoming as the private keys described above in that the public keys are recipient specific and not application specific. For instance, assume that a physician has access to several different application programs at a medical facility and that, at two different times, the physician uses first and second different application programs, respectively, to access a first patient record that is stored in Felsher's database 6 (see Felsher's Fig. 1). Here, according to Felsher, when the physician requests the first patient record using the first application program, server 5 uses a public key associated with the first physician to encrypt the requested record and transmits the encrypted record to the physician.

When the physician requests the first patient record using the second application program, the server 5 again uses the public key associated with the first physician to encrypt the requested record. The public key used to encrypt in this second case where a second application program is used to access the first record is the same as the public key used to encrypt in the first case where the first application program was used to access the first record. In fact, irrespective of which application program the physician uses to access the first patient record, the same public key is used to encrypt and therefore, even when encrypted, a system wide patient identification number (e.g., a SS number) will include the same information when transmitted to the first physician.

As another instance, assume that two different physicians use a single application program at different times to access the first patient record. Here, according to Felsher where public keys are recipient distinct as opposed to application distinct, despite the fact that one application program is used to access the first patient record, when the first physician accesses the first patient record the server uses a first public key associated with the first physician to encrypt the first patient record and when the second physician accesses the first patient record the server uses a second public key

associated with the second physician to encrypt the first patient record and each of the encrypted records includes an encrypted patient ID that is distinct.

Thus, in short, like the private keys, Felsher's public keys are recipient (i.e., medical professional) specific and not application specific or, for that matter, patient specific.

Moreover, Applicant adds that the encryption and decryption processes described in Felsher comprise a single application and not network applications (plural) and that, where multiple applications occur in Felsher, patient identification numbers are uniform system wide for each patient. To this end, Felsher teaches at paragraph 266 that system wide patient identification numbers are employed such as social security numbers or surrogates therefore which would also be system wide numbers for patients. To transmit patient identification numbers between application programs in a secure and private manner, those numbers, as part of a patient record, are encrypted, transmitted and decrypted. Nevertheless, patient identification numbers stored by the central server 3 prior to encryption and the identification numbers used by the end application programs after decryption are identical (i.e., may be SS numbers) and what happens in between the server and the application programs is wholly part of a single encryption/decryption program or process.

Turning to Moragne, Moragne fails to teach what Felsher lacks with respect to claim 1. More specifically, Moragne fails to teach or suggest a system wherein an exchange server maintains a list of applications and application specific patient identification numbers.

For all of the above reasons Applicant believes claim 1 and claims that depend there from are patentably distinct over the cited references and allowance of the same is requested.

7. Claim 5 includes limitations similar to the limitations of claim 1. For at

least the above reasons Applicant believes claim 5 and claims that depend there from are distinct over the references cited and requests that the rejections be withdrawn.

### **Response To Arguments**

In this section of the Office Action the Examiner indicates that Applicant's response was not persuasive because the reference table claimed was suggested by Felsher. Applicant strongly disagrees. Here the Office Action states that Felsher's private key is a form of application distinct identification number and that the applet is a form of an application program and that the applet is considered to be recipient distinct because it is configured via a user specific private key to decrypt a specific patient medical record.

As explained above, Applicant admits that Felsher's private key is in fact recipient distinct as that key is unique to a specific recipient (e.g., a medical professional). However, as discussed above, the recipient distinct keys are not application distinct patient identification numbers as required by the claims of the present application. Thus, for instance, irrespective of which application is being used by a medical professional to access a record, the medical professional's private key will always be the same in Felsher and there is no teaching or suggestion in Felsher to the contrary (see paragraph 269 that teaches that each medical professional may be provide his own public/private key pair).

Moreover, Felsher only teaches that the private key is stored at a user's computer or application and never teaches or even remotely suggests that the private key may be stored at a central type exchange server (indeed, private means private to the individual which is contrary to the notion that the private key may be stored at a central exchange server). Thus, Felsher's private key is not application specific and the private keys are not stored at a central exchange server and for at least these two reasons the private key cannot read on the claimed application distinct patient identification number reference table.

With respect to the applet, the applet is not recipient distinct. Felsher makes



clear, as explained above, that the applet is simply a program needed to open a record after the record is sent (see second last sentence in paragraph 252) and that the applet is not patient or application distinct. Here, as taught by Felsher, a record is wrapped with an applet and then encrypted with a recipient's public key prior to transmission to a patient (see last sentence in paragraph 260). Once the encrypted record and applet are received, a patient's private key is used to decrypt the record and applet and after decryption, the applet is activated to provide access to the content of the record (see paragraph 228). Thus, the private key and the applet operate in sequence, not in parallel, to provide access to the record content.

Regarding whether or not it would have been obvious to have separate identification numbers for each application used to access each individual medical record, Applicant is not claiming this limitation. Instead, Applicant is claiming a reference table stored by a single server that includes a list of network applications and patient identification numbers for each of the applications in the list where the patient identification numbers are application distinct. Thus, Applicant is claiming a system including a table that includes application distinct and patient distinct patient identification numbers.

In the event that the Examiner maintains that the private key is application distinct and/or that the applet is recipient distinct, Applicant requests that the examiner indicate more clearly where Felsher even suggests such teachings. To this end, paragraphs 222, 230, 248, 252, 266 and 279 appear to be completely consistent with Applicant's understanding of Felsher as a whole as described above.

With respect to paragraph 269 in Felsher, Applicant notes the following. Felsher's paragraph 269 teaches that each medical professional may be provided with a public key/private key pair. Here, as indicated above, Felsher's private keys are private and hence stored at recipient computers and not on an exchange server. Felsher's public keys may be stored at a single server but they are not unique to applications or specific patients. Thus, for instance, Felsher's public key for a first medical professional will be the same regardless of which of ten patients the

professional is seeking a record for. Similarly, Felsher's public key for a first medical professional will be the same regardless of which application the first medical professional is using to access information.

With respect to Felsher's applet being an application program, as indicated above, Applicant has examined Felsher in detail and has been unable to locate even a single teaching or suggestion that Felsher's applets are different for different records. Instead, Felsher appears to teach a single applet for all records. Thus, Felsher's applet, even if it is considered an application, does not comprise multiple different applications or a plurality of applications as required by the preambles of claims 1 and 5.

Applicant has added new claims 14 through 18 that are method claims that are similar to the system claims in claims 1-8.


Carl Dvorak  
Serial No.: 10/052,659  
Office Action Response  
Page 16

Applicant has introduced no new matter in making the above remarks. In view of the above remarks and amendments, Applicant believes claims 1-8 and 14-18 of the present application recite patentable subject matter and allowance of the same is requested. No fee in addition to the fees already authorized in this and accompanying documentation is believed to be required to enter this amendment, however, if an additional fee is required, please charge Deposit Account No. 17-0055 in the amount of the fee.

Respectfully submitted,

CARL DVORAK

Date: 9-5-07

By:   
Michael A. Jaskolski  
Reg. No. 37,551  
Attorney for Applicant  
QUARLES & BRADY, LLP  
411 East Wisconsin Avenue  
Milwaukee, WI. 53202-4497  
(414) 277-5711